EXHIBIT A

Dockets.Justia.com

New Jersey Turnpike Authority

Information Security Policy

Table of Contents

Introduction 1

Classification of NJTA Information 1

Scope 1

Relation to HIPAA Privacy and Security Rules 2

Information Security Responsibilities 2
- A. General Security Responsibility for Users 2
- B. Information Owners Responsibilities 2
- C. TAS Department Responsibilities 3
- D. Human Resources Responsibilities 3

Information Security Practices 3
- A. User-ID Guidelines 3
  - 1. Temporary User-Ids 3
- B. Password Guidelines 3
- C. Password Standards 4
  - 1. Password Length 4
  - 2. Password Expiration 4
  - 3. Incorrect Password Guesses 4
  - 4. Assignment of Initial Passwords 4
  - 5. Password Reset Administration 4
  - 6. Display and Printing of Passwords 4
- D. Restrictions of Special System Privileges 5
- E. Use and Distribution of Powerful Security Tools 5
- F. Internal Reporting of Data Security Violations 5
- G. Data Storage and Back-ups 5
- H. Handling of Sensitive/Confidential Types of Information 5
  - 1. Disposal of Critical and Confidential Data 5
  - 2. Dealing with Critical and Confidential Information 5
- I. Computer Viruses 5
- J. Personal Computer Usage 6
  - 1. Privacy and Content 6
  - 2. Software Installations 6
  - 3. Software Licenses 6
- K. Remote Access Restrictions 6
  - 1. Remote Access Privileges 6
  - 2. Dial-up Guidelines 6
  - 3. Individual Modem Usage 7
- L. Electronic Mail Guidelines 7
  - 1. Overview 7
  - 2. Privacy and Content 7
  - 3. Reporting of Violations 7
  - 4. Email Retention 8

M. Internet Access Guidelines 8
1. Overview 8
2. Internet Security 8
3. Software and File Downloads 8
4. Privacy and Content 8
5. Reporting of Violations 9

Appendix A - Glossary 10

Appendix B - Password Do's and Don'ts 12

Appendix C – Documents and Forms 13

Case 2:33-av-00001 Document 1366-2 Filed 05/22/2007 Page 4 of 20

INTRODUCTION

New Jersey Turnpike Authority (NJTA) makes use of a variety of computer equipment, applications, files, databases and other resources that support NJTA's business on a daily basis. Therefore, it is necessary to develop and enforce security measures to protect NJTA's information from unauthorized disclosure, modification, misuse, and deletion. It is important to ensure that the level of protection is adequate to ensure the continued availability and integrity of the information produced from information systems, and information received from third parties, whether electronic or paper.

The information tools and resources of NJTA are made available to users for business purposes only. Because NJTA's computer and communications systems are to be used for business purposes only, employees have no right to privacy in their e-mail, voice mail, Internet usage, or desktop computers.. Users may be disciplined for misuse or personal use of NJTA's information systems.

It is the responsibility of all users to read and comply with this document. Compliance with the policies set forth in this document is essential, and a requirement for continued employment at NJTA. Non-compliance with this policy will result in disciplinary action, including termination, civil or criminal legal action. NJTA reserves the right to revoke the privileges of any user at any time. All users are responsible for adhering to copyright, patent laws, and license agreements for intellectual property (such as NJTA's or a third-party's software). Violations of authorial integrity may be grounds for sanctions; examples of such violations include: plagiarism, invasion of privacy, unauthorized access, trade secret exposure, and copyright violations. If you have any questions regarding the information security policies, responsibilities, or procedures, you should contact the Director of TAS (Technology & Administrative Services).

CLASSIFICATION OF NJTA INFORMATION

All NJTA information resources, electronic or paper, are considered important and critical. Appropriate controls are in place, automated and/or manual, for protecting NJTA resources. Also, certain information sensitive in nature, such as payroll and benefits, customer and contract information, will be considered confidential information of the NJTA.

SCOPE

This policy becomes effective upon its issuance and covers all information systems and related activities of NJTA. Items covered include, but are not limited to, mini-computers systems, communication systems, file server, networks, personal computers and all forms of data including text, video, audio, imagery, and other representations used as information or in control functions. Data may reside in any form or media, including human and machine readable, such as paper documents, photographs, magnetic disks and tapes, optical disks, video displays, audio forms, electrical signals, radio-frequency signals, and optical signals.

All users of NJTA information systems will be covered under this policy. Users include NJTA employees, officers, directors, agents, associates, consultants/contractors, vendors, temporary help, and third party processors of NJTA data.

The purpose of the policy is to protect information assets from unauthorized disclosure, modification, misuse, and deletion and to protect the Authority from legal liability. All employees and consultants/contractors shall understand and agree to abide by the NJTA Information Security Policy.

RELATION TO HIPAA PRIVACY AND SECURITY RULES

Relative to the security of employee medical information, specifically that information defined as Protected Health Information (PHI) under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the promulgated HIPAA Privacy and Security Rules are hereby incorporated by reference. In all matters pertaining to the privacy and security of PHI, the provisions of the HIPAA rules shall take precedent over any similar or contradicting provisions herein. Any questions relative to the HIPAA rules should be addressed to the New Jersey Turnpike Authority's HIPAA Privacy Officer.

INFORMATION SECURITY RESPONSIBILITIES

All users (as defined under the section 'Scope') of NJTA equipment, resources or information, will comply with the provisions of this information security policy. Non-compliance with information security policies, practices and procedures is considered unsatisfactory and subject to disciplinary action. Certain specific responsibilities are as follows:

A. General Security Responsibility for Users

All users should understand and comply with the provisions of this information security policy, which will be acknowledged by the virtue of their employment. Users shall maintain the privacy and confidentiality of information regardless of form, i.e., electronic or paper. Users will be responsible for activities associated with their passwords, and therefore, passwords must be kept confidential. Passwords should not be easily guessed (see section *B. 'Password Guidelines'* for details). Individuals should not divulge their passwords to any other individual for any reason. All passwords should be promptly changed if they are suspected of being disclosed, or known to have been disclosed to unauthorized parties. However, there may exist special circumstances under which an individual chooses to share their password with another individual for business purposes. When this occurs, the owner of the password must change their password as soon as possible. The owner of the ID and password is accountable for all activities associated with their ID and password.

Users should not leave personal computers, workstations, or terminals unattended without first logging-out or locking the session, especially if working on sensitive, valuable, or confidential information. Any suspected information security problems and/or violations should be reported to the Human Resources and TAS Departments. Users will not test, or attempt to compromise access controls.

B. Information Owners' Responsibilities

Information Owners (Department Managers) will authorize and approve access to NJTA's information systems for resources and employees under their responsibility. Using the NJTA's *Network Access Request Form*, (Appendix C) Department managers may request to grant new/additional or remove/deny privileges and rights to access certain information. Access to information will be based on the 'need-to-know' basis, i.e., necessary to perform job duties. All significant changes in user (employees, consultants/contractors) duties or employment status will be promptly reported to the Human Resources Department. Changes in job function and employment status are conveyed to TAS via copies of Payroll Change Notices. In addition, Information Owners will ensure that all NJTA computing property is returned when an employee, or consultant/contractor relationship under their control is terminated with NJTA. Information Owners are responsible for promptly reporting any noted variances from this policy to the Human Resources Department.

C. TAS Department Responsibilities
The TAS Department will perform the responsibilities of custodian over the information and information systems. This includes defining and maintaining the integrity of specific control procedures, implementing and maintaining cost-effective information control measures, and providing back-up and recovery capabilities. In addition, TAS will ensure that adequate information security controls are part of the systems development process and that security of programs, data, functionality, platforms and network access are in agreement.

D. Human Resources Responsibilities
The Human Resources department will notify the TAS Department on a timely basis of all new hires, terminations, promotions, demotions, reassignments, leaves of absence, short or long term disability, or other significant changes in status that might require a change in information access privileges.

INFORMATION SECURITY PRACTICES

A. User-ID Guidelines
User-IDs and passwords will be used to control access to all NJTA computer systems and networks. Each User-ID must represent only one employee, and employees must not share User-IDs. Exceptions to this rule will be allowed in some cases if approved by TAS. User-IDs will be re-validated annually by each information resource owner to ensure that they are still required. To ensure individual accountability, the definition of all users and jobs through access controls is mandatory. Default User-IDs are not allowed. All requests for User-Ids will be made using the *Network Access Request Forms*. (See Appendix C).

1. Temporary User-IDs:
Temporary User-IDs are sometimes granted to external "users" such as consultants, external vendor's personnel, temporary employees, etc. Special controls are used to provide the prompt suspension/deletion of a temporary User-ID when the contract expires. A default expiration period is defined by the requesting department manager and applied to all temporary User-IDs. Such temporary User-IDs will automatically expire at specified time.

B. Password Guidelines
The most vulnerable part of any computer system is the user password. Any computer system –no matter how secure it is from network or dial-up attack, and other threats– can be fully exploited by someone who can gain access via a poorly chosen password. If passwords are to withstand attacks and protect the system, they should be constructed with care. Guessing passwords is a popular and often successful attack method by which unauthorized persons gain system access. Passwords should not include: your name, your User-ID, your spouse's name, your address, easily guessed personal facts, and anything to do with NJTA. For example, a poor choice of password for users at NJTA would be "plaza9", "tickets", etc. The password should be something memorable, but not trivial. An alphanumeric combination is suggested.

A password serves as the access key to NJTA's computer systems, thus it should be protected accordingly. Passwords should not be written down, stored in readable form in batch files, automatic log-on scripts, software macros, terminal function keys, or in other locations where unauthorized persons could discover them, such as under keyboards or behind desk calendars. It is important to prevent passwords from falling into the wrong hands. As previously stated, the owner of the ID and password is accountable for all activities associated with their ID and password.

(See *Appendix B* for the DOs and DON'Ts on password security.)

C. Password Standards

1. Password Length:

Another important consideration in password construction is length. The length of the password is important because the longer it is, the harder it should be for someone to guess it. Password length is checked by the system at the time it is chosen. You will be denied a password if it is too short. For primary access points of computer systems at NJTA, the minimum password length will be six (6) alpha-numeric characters.

2. Password Expiration:

Effectiveness of passwords diminishes over time due to various reasons (such as a co-worker might have seen your password as you typed it in), and thus, should be periodically changed. For the primary access points of computer systems at NJTA, system forced password change intervals will be set for ninety (90) days. When keying in the password, users will ensure that no one is directly observing it. The password should be changed immediately if it may have been exposed.

3. Incorrect Password Guesses:

Also, to prevent password guessing attacks, the number of consecutive attempts to enter an incorrect password is limited where technically possible. After three (3) unsuccessful attempts to enter a password within 15 minutes, the account will be disabled for 30 minutes. If dial-up or other external network connections are involved, the caller will be disconnected. After 30 minutes, the user has another 3 attempts to logon. The involved User-ID can be reset by a system administrator.

4. Assignment of Initial Passwords

The initial passwords issued by a security administrator will be valid only for the involved user's first on-line session where technically possible. At that time, the user will be forced to choose another password before any other work can be done.

5. Password Reset Administration

If a password is forgotten, or for some reason a user cannot change it, the TAS Department must be contacted. An employee shall be positively identified in order to obtain a new or changed password. Passwords that are reset or created for an employee by the TAS Department shall be set to an expired value, where technically possible, so that the employee must change the password on first use.

6. Display and Printing of Passwords

The display and printing of passwords will be masked, suppressed, or otherwise obscured, where technically possible, such that unauthorized parties will not be able to observe or subsequently recover them.

D. Restrictions of Special System Privileges

Special system privileges, such as the ability to examine the files of other users or bypass system security is restricted to those who are directly responsible for system management and/or security. Exceptions may be made that allow managers to see files of subordinates as requested.

E. Use and Distribution of Powerful Security Tools

Use of vulnerability identification software or other tools that could be used to compromise the security of information systems is prohibited unless expressly approved by the TAS Department.

F. Internal Reporting of Data Security Violations

Users should report violations to the TAS Department as soon as possible so that corrective action may be taken. Possible violations include, but are not limited to suspected compromise or disclosure of confidential information, passwords, and system controls. Violations of the *Information Security Policy* and theft or loss of any information or equipment should also be reported. Note that problems such as computer viruses and other computer problems should be reported to the TAS Department.

G. Data Storage and Back-ups

All NJTA information which is stored on network file servers is backed-up nightly and securely retained so that information can be restored with minimum loss in the event of a disaster or corrupted information. Redundant back-ups are stored off-site for use in disaster recovery scenarios. It is important to note that individual user's PCs are not backed up. Storing critical business data on local hard drives greatly increases the exposure for data loss as well as security breaches.

H. Handling of Critical/Confidential Types of Information

1. Disposal of Critical and Confidential Data

Any information that is considered confidential (as defined by department managers) should not be left in areas where it might be observed or discovered by unauthorized individuals. This includes storage media (like floppy diskettes, CD-ROMs, computer tapes, etc.) that are currently being used, or discarded storage media.

All critical and confidential information on computer related media should be disposed of properly. Since deletion methods vary based on the type of media used, please refer to the TAS Department as the need arises.

2. Dealing with Critical and Confidential Information

Special care must be used when handling sensitive forms and system output. Special forms, such as blank checks, must be kept secure from unauthorized individuals. The sequence of the checks should be logged before and after a print run. When the output is ready for distribution, it must only go through management approved distribution channels. An audit trail should be created to ensure that the output reaches its desired destination.

I. Computer Viruses

Computer virus programs are designed to perform undesirable results. Controls (like implementation of anti-virus software) shall be applied by TAS to reduce the risk of damage by these programs. These controls are designed to prevent infection and to disinfect damaged programs, files and data. Users will not use any externally provided software unless inspected and installed by the TAS Department. Virus checking is done automatically without user intervention on all systems on which virus checking is possible.

J. Personal Computer Usage

All Personal Computers, peripherals, etc. remain the property of NJTA, and all data contained thereon must conform to all NJTA policies and standards. As such, all information remains the property of NJTA and NJTA reserves the right to monitor and inspect said property at any time without prior notification.

1. Privacy and Content

The employee has no expectation of privacy relative to any information, including email, stored on any NJTA computers, peripherals, devices or networks. Users may not transfer, receive or store any software or information that contains any language/material content that may be reasonably considered offensive or disruptive to any employee. Offensive content would include, but would not be limited to, sexual comments or images, racial slurs, gender-specific comments or any comments that would offend someone on the basis of their age, race, sexual orientation, religious beliefs, political beliefs, national origin, or disability.

2. Software Installations

Users are prohibited from installing any software without prior approval from the TAS Department. This applies to all software including additional screen savers, games, wallpaper, bitmaps, etc. Windows operating systems, as configured by the TAS Department, are installed with a wide variety of these utilities and additional installations are prohibited. Any and all applications, programs, games, screen savers, files, etc., stored or loaded on NJTA equipment found to be in violation of the *New Jersey Turnpike Authority Information Security Policy* or any other NJTA policies, will be promptly removed and deleted without prior notification. Such violations will then be reported to the Director of TAS.

All installations by vendors, consultants, business partners, etc., must be done with prior approval and in conjunction with the TAS Department. Users requiring application software for the conduct of legitimate NJTA business, which was not originally provided, must provide written notification to the TAS Department. Upon completion of compatibility testing and approval, the TAS Department will subsequently install all legitimately, licensed software.

3. Software Licenses

All application software used by NJTA employees, or on any NJTA equipment, must be legitimately purchased, licensed and registered with the TAS Department. Users are forbidden from installing, copying or distributing software in any form.

K. Remote Access Restrictions

1. Remote Access Privileges

Remote Access will be granted only upon authorization from the Director of TAS. Continuation of all remote access accounts will be reviewed annually by the TAS Department.

2. Dial-Up Guidelines:

Dial-up telephone lines by their very nature are inherently non-secure and as such increase the risks of a security breach. Third-party vendors applying maintenance to NJTA software systems will only be given dial-up maintenance privileges when approved by the TAS Department based on a bona fide need. These privileges will be enabled only for the time period needed to accomplish the approved tasks. Dial-up access will be controlled via system level authentication techniques. Under no circumstances may information regarding NJTA's dial-up instructions and computer phone numbers be posted on electronic bulletin boards, listed in phone directories, or revealed to any unauthorized parties.

3. Individual Modem Usage:

NJTA will strictly control the use of modems. Modems installed on workstations will not be used for dial-up activities into the NJTA network. These modems are not permitted to provide dial-in capabilities and shall not answer incoming calls. Authorized modem usage shall be for bona-fide business purposes only. The TAS Department shall annually review all modem installations.

L. Electronic Mail Guidelines

1. Overview

NJTA maintains, as part of its technology platform, an electronic-mail system, Microsoft Exchange. This system is provided to assist in the conduct of Authority business. All computers, and the data stored on them, are and remain at all times the property of NJTA. As such, all electronic-mail messages composed, sent and received are and remain the property of NJTA.

2. Privacy and Content

NJTA monitors and filters all electronic mail activity. The user has no privacy rights relative to electronic mail.

Electronic mail messages may not contain language/material content that may be reasonably considered offensive or disruptive to any employee. Offensive content would include, but would not be limited to, sexual comments or images, racial slurs, gender-specific comments or any comments that would offend someone on the basis of their age, race, sexual orientation, religious beliefs, political beliefs, national origin, or disability.

Electronic mail will be limited to the conduct of NJTA business. Propagation of "chain letters" is prohibited. Unsolicited mail is unwelcome and should be immediately deleted without being opened. Transmission of graphics (JPEG, GIF) is prohibited unless it is done so in the conduct of legitimate NJTA business. Please note that even after a message is deleted, it can be recreated.

3. Reporting of Violations

Employees learning of any misuse of the electronic-mail system or violations of this policy shall notify in writing the Director of TAS and copy the Director of Human Resources.

Use of electronic mail is a privilege, which can and will be revoked at any time for violation of the policy. This revocation could have an impact on job performance. Violations of this policy will be dealt with promptly and are subject to disciplinary actions. Violation of the Electronic-Mail Policy and Standards may result in suspension or loss of Electronic mail access and disciplinary action up to and including termination of employment and legal action.

See *Appendix C* for **Electronic Mail Form**

4. E-Mail retention

In its native form, all email messages are stored on NJTA file servers. In order to maintain file server efficiencies, all email should be periodically purged or archived by the user to their network drive. All emails that enter or leave our system are archived to DVD.

M. Internet Access Guidelines

1. Overview

New Jersey Turnpike Authority maintains, as part of its technology platform, the ability to access the Internet. This capability is provided solely to assist in the conduct of NJTA business. As with the telephone and fax machines, the Internet can be used for limited incidental personal use that does not interfere with work duties. More than limited incidental personal use may subject an employee to discipline or removal of Internet access. Continuing use of the Internet is dependent on compliance with all NJTA use policies. NJTA cannot and will not be held accountable for information that is retrieved from the Internet. NJTA reserves the right to monitor Internet activities for usage and content at any time. The user has no privacy rights relative to Internet usage.

2. Internet Security

All users of the Internet must be authorized by the Deputy Executive Director via a request to TAS. This request consists of a "Network Access Request Form" for an Internet Account *(see Appendix C)* and an attached justification memorandum. Upon approval, the Internet account will be implemented by the TAS Department. Without prior approval, access will be denied. All network Internet connections originating at NJTA pass through an approved firewall. The firewall monitoring software tracks all connections and identifies them by User-Id.

3. Software and File Downloads from the Internet

User will not download or upload any NJTA information, data, software, etc., which does not comply with NJTA policies and copyright or licensing agreements. Installing of Internet software (including shareware and freeware) without prior authorization from the Director of TAS is prohibited. (See section *J. Personal Computer Usage*)

4. Privacy and Content

Access to the Internet may not contain language/material content that may be reasonably considered offensive or disruptive to any employee. Offensive content would include, but would not be limited to, sexual comments or images, racial slurs, gender-specific comments or any comments that would offend someone on the basis of their age, sexual orientation, religious beliefs, political beliefs, national origin, or disability. Users will not post, mail, upload or broadcast any sort of information for personal use or gain. Use of fee-for-service providers on the Internet is not allowed without prior, necessary approvals.

When using the Internet, individuals should identify themselves properly. Users should be careful about how they represent themselves, given that what they say or do could be interpreted as an opinion or policy of NJTA. Users should be aware that their conduct could reflect on the reputation of NJTA. Users should handle Internet queries about NJTA matters that are outside of their immediate scope of work in the same manner that they would handle telephone inquiries.

When there is evidence that an employee is involved in activities that are prohibited by law, that violate state regulations, that use abusive or objectionable language in either public or private messages, that might jeopardize the technical systems of NJTA or that violate this or other NJTA policies and guidelines, all monitors and logs will be made available to the Human Resources Department and/or any other agencies or authorities as required.

5. Reporting of Violations

Individuals learning of any misuse of Internet access or violations of this policy shall notify in writing the Director of TAS and copy the Director of Human Resources.

Access to the Internet is a privilege, which can and will be revoked at any time for violation of this or any other NJTA policies. Violations of this policy will be dealt with promptly. Violations may result in suspension or loss of Internet access and disciplinary actions up to and including termination of employment and legal action.

See *Appendix C* for Internet Authorization Request Forms.

APPENDIX A GLOSSARY

ACCESS CONTROL: Usually a software based control that is designed to prevent unauthorized access to data, or use of system functions and programs.

APPLICATION: A specific task-oriented program that is designed to suit employee needs.

AUTHORIAL INTEGRITY: The integrity associated with any proprietary (NJTA owned or third-party owned) asset such as a computer program.

DATABASE: A systematic collection of data elements that are organized according to a specific design that can be hierarchical or relational.

FIREWALL: A hardware and software solution that would be placed between a trusted network and a public network so as to provide protection from unauthorized access.

HARDWARE: Computer peripherals, or telecommunications devices used for processing information assets.

LAN: A Local Area Network; a high-speed pathway between computers and equipment that provides resources, data, and program sharing or exchange.

LOG-ON/LOG-OUT: The process of establishing or terminating a session with a computer, and identifying yourself as an authorized user by entering a User-ID and a password.

MAGNETIC TAPE: Magnetically covered plastic ribbon that is used to store information.

MAINFRAME: A large general-purpose computer that stores many of the firm's applications.

MODEM: A device that encodes data for transmission over a particular medium, such as telephone lines, coaxial cables, fiber optics, or microwaves.

INFORMATION OWNER: The designated person, or area, that is responsible for the integrity of a set of information. The owner determines the level of access control to the information within the parameters of company policies.

PASSWORD: A confidential and unique character string that is used to verify the identity of an employee.

REMOTE ACCESS: Sending and receiving data to and from a computer, or controlling a computer with terminals or Personal computers connected through communications (i.e. phone) links.

SECURITY VIOLATION: Any incident or situation, which violates or compromises the Information Security Policy.

SOFTWARE: An entire set of programs, procedures, and related documentation associated with an application designed to be run on a computer system. The software may be either developed or acquired by the company.

USER-ID: User Identification; a unique identifier assigned to each authorized user.

VIRUS: A computer program that automatically copies itself, thereby "infecting" other disks or programs without the user knowing it, and then plays some kind of trick or disrupts the operation of the computer; knowingly spreading a computer virus is a crime under common law and under specific laws in various states.

WORKSTATION: A high performance microcomputer that has been specified for graphics, CAD, CAE or scientific applications; (at NJTA Industries, workstation and PC are used interchangeable).

APPENDIX B PASSWORD DOs AND DON'Ts

Password Security	
DOs	**DON'Ts**
Do use a password with mixed-case alphabetic characters for your PC. (VAX passwords are not case-sensitive).	**Don't** use your User-ID name in any form (e.g., as-is, reversed, capitalized, doubled)
Do use a password with some non-alphabetic characters (e.g., digits)	**Don't** use a password made of all digits, or all the same letter
Do give password crackers a hard time	**Don't** use your first, middle, or last name in any form
Do use a password that is memorable, but not trivial.	**Don't** use your spouse's, child's, or pet's name
Do use passwords that are derived from pass phrases (e.g., PemdAS for "Please excuse my dear Aunt Sally")	**Don't** use a word contained in English or foreign language dictionaries, spelling lists, or other common lists of words
Do use a password that is long enough to confound brute force attacks	**Don't** use a password shorter than six characters
Do use a password that you can type quickly, without having to look at the keyboard	**Don't** use other information easily obtained about you (e.g., license plate numbers, telephone numbers, social security numbers, automobile type, name of your street)
Do memorize you password	**Don't** write your password down, store it as a function key, or a macro
Do keep your password private	**Don't** give your password to anyone
Do lock or log-out of the system when you must step away from your computer	**Don't** leave your computer terminal unattended with your User-ID, and password still active

Appendix C Forms and Applications

This section contains a copy of pertinent forms and applications. Please copy and use these forms when filing requests. Please read all forms very carefully as they contain the specific policies for the use of these resources. Signed documents must be returned to the TAS Department for processing and filing.

Electronic Mail Form is used to assure compliance with NJTA policies.

Internet Access Request Form is used when requesting the privileges to access the Internet/World Wide Web.

Network Access Request Form is used to request new User-Ids for all new employees (including part time, temporary, vendors, etc.). This form is also required when granting/denying additional network access to current users.

Electronic Mail Form

1. Overview
NJTA maintains, as part of its technology platform, an electronic-mail system. This system is provided to assist in the conduct of Authority business. All computers, and the data stored on them, are and remain at all times the property of NJTA. As such, all electronic-mail messages composed, sent and received are and remain the property of NJTA.

2. Privacy and Content
NJTA monitors and filters all electronic mail activity. The user has no privacy rights relative to electronic mail.

Electronic mail messages may not contain language/material content that may be reasonably considered offensive or disruptive to any employee. Offensive content would include, but would not be limited to, sexual comments or images, racial slurs, gender-specific comments or any comments that would offend someone on the basis of their age, sexual orientation, religious beliefs, political beliefs, national origin, or disability.

Electronic mail will be limited to the conduct of NJTA business. Propagation of "chain letters" is prohibited. Unsolicited mail is unwelcome and should be DELETED UNOPENED. Transmission of graphics (JPEG, GIF) is prohibited unless it is done so in the conduct of legitimate NJTA business. Please note that even after a message is deleted, it can be recreated.

The NJTA provides computers, computer files, and the electronic mail (e-mail) system to assist you in completing your job duties as quickly and efficiently as possible. This equipment and any other informational, storage, or retrieval services that the NJTA provides is to be used for business purpose only. Consequently, use of these facilities for personal reasons is strictly prohibited and all computer pass codes must be available to the NJTA at all times. Failure to follow these rules can lead to discipline up to and including discharge. The NJTA reserves the right to enter, search, and monitor the computer files or e-mail of any employee, without advance notice. Such action may be taken by the NJTA for any purpose.

3. Reporting of Violations
Employees learning of any misuse of the electronic-mail system or violations of this policy shall notify in writing the Director of TAS and copy the Director of Human Resources.

Use of electronic mail is a privilege, which can and will be revoked at any time for violation of the policy. Violations of this policy will be dealt with promptly and are subject to disciplinary actions. Violation of the Electronic-Mail Policy and Standards may result in suspension or loss of Internet access and disciplinary action up to and including termination of employment and legal action.

4. EMail retention
In its native form, all email messages are stored on NJTA file servers. In order to maintain file server efficiencies, all email should be periodically purged or archived by the user.

Use of electronic mail is a privilege, which can and will be revoked at any time for violation of the policy. Violations of this policy will be dealt with promptly and are subject to disciplinary actions. Violation of the Electronic-Mail Policy and Standards may result in suspension or loss of E-mail access and disciplinary action up to and including termination of employment and legal action.
NJTA reserves the right to change this policy at any time with or without notice.

VIOLATION OF THE E-MAIL POLICY AND STANDARDS MAY RESULT IN SUSPENSION OR LOSS OF ELECTRONIC MAIL AND DISCIPLINARY ACTION UP TO AND INCLUDING TERMINATION OF EMPLOYMENT AND LEGAL ACTION.

I have read the E-Mail Policy and Standards and, in signing below, agree to abide by them.

Signature______________________ Date ______________

Please Print ______________________ Dept ______________
(name)

Return to: TAS Department for Inclusion in Human Resource File.

Internet Access Request Form

1. Overview
New Jersey Turnpike Authority maintains, as part of its technology platform, the ability to access the Internet. This capability is provided solely to assist in the conduct of NJTA business. Continuing use of the Internet is dependent on compliance with all NJTA use policies. NJTA cannot and will not be held accountable for information that is retrieved from the Internet. NJTA reserves the right to monitor Internet activities for usage and content at any time. The user has no privacy rights relative to Internet usage.

2. Internet Security
All users of the Internet must be approved by the Deputy Executive Director via a request to TAS. Without proper approval, access will be denied. Upon approval, the Internet account will be implemented by the TAS Department. All network Internet connections originating at NJTA pass through an approved firewall. The firewall monitoring software tracks all connections and identifies them by User-Id.

3. Software and File Downloads from the Internet
User will not download or upload any NJTA information, data, software, etc., which does not comply with NJTA policies and copyright or licensing agreements. Installing of Internet software (including shareware and freeware) without prior authorization from the Director of TAS is prohibited. (see section *J. Personal Computer Usage*)

4. Privacy and Content
Access to the Internet may not contain language/material content that may be reasonably considered offensive or disruptive to any employee. Offensive content would include, but would not be limited to, sexual comments or images, racial slurs, gender-specific comments or any comments that would offend someone on the basis of their age, sexual orientation, religious beliefs, political beliefs, national origin, or disability. Users will not post, mail, upload or broadcast any sort of information for personal use or gain. Use of fee-for-service providers on the Internet is not allowed without prior, necessary approvals.

When using the Internet, individuals should identify themselves properly. Users should be careful about how they represent themselves, given that what they say or do could be interpreted as an opinion or policy of NJTA. Users should be aware that their conduct can reflect on the reputation of NJTA. Users should handle Internet queries about NJTA matters that are outside of their immediate scope of work in the same manner that they would handle telephone inquiries.

When there is evidence that an employee is involved in activities that are prohibited by law, that violate state regulations, that use abusive or objectionable language in either public or private messages, that might jeopardize the technical systems of NJTA or that violate this or other NJTA policies and guidelines, all monitors and logs will be made available to the Human Resources Department and/or any other agencies or authorities as required.

The NJTA provides computers, computer files, and the electronic mail (e-mail) system to assist you in completing your job duties as quickly and efficiently as possible. This equipment and any other informational, storage, or retrieval services that the NJTA provides is to be used for business purpose only. Consequently, use of these facilities for personal reasons is strictly prohibited and all computer pass codes must be available to the NJTA at all times. Failure to follow these rules can lead to discipline up to and including discharge. The NJTA reserves the right to enter, search, and monitor the computer files or e-mail of any employee, without advance notice. Such action may be taken by the NJTA for any purpose.

ACCESS TO THE INTERNET IS A PRIVILEGE WHICH CAN AND WILL BE REVOKED AT ANY TIME FOR VIOLATION OF THIS POLICY. VIOLATIONS OF THIS POLICY WILL BE DEALT WITH PROMPTLY. VIOLATIONS MAY RESULT IN SUSPENSION OR LOSS OF INTERNET ACCESS AND DISCIPLINARY ACTIONS UP TO AND INCLUDING TERMINATION OF EMPLOYMENT AND LEGAL ACTION.
NJTA RESERVES THE RIGHT TO CHANGE THIS POLICY AT ANY TIME WITH OR WITHOUT NOTICE.

Internet Access Request Form (page 2)

I have read the Internet/E-Mail Policy and Standards and, in signing below agree to abide by them. Please keep a copy for your files and forward the original to the TAS Department.

Signature______________________________ Date ____________________

Please Print ______________________________ Dept ____________________
(name)

Return to TAS Department for Inclusion in Human Resource File

NETWORK ACCESS REQUEST FORM

Date: ______________________

Please fill out accordingly and forward to the TAS Dept for review/implementation.

New User/ Applicant's Name:		Employee Number:	
Title:		Dept:	
Supervisor:		Dept. Head:	

If this user is to be set up identically to another existing user, please enter that user's name: ______________________

If this is a customized request, please check below what is needed:

- ☐ VMS Alpha Account
- ☐ VMS VAX Account
- ☐ Windows NT Account
- ☐ Internet Account (Please attach justification memorandum)
- ☐ Remote Dial-In Account (Please attach justification memorandum)
- ☐ Commercial Software Product:
  - ☐ Word
  - ☐ Excel
  - ☐ PowerPoint
  - ☐ Access
  - ☐ Other: ______________________

- ☐ Access to existing applications (Please specify) ______________________
- ☐ New application (Please describe briefly)______________________
- ☐ Printer (type and location) ______________________
- ☐ Workstation
- ☐ Laptop Computer
- ☐ Other: ______________________

____

Department Head or Manager's Signature

Please keep a copy for your files and forward the original to the TAS Department.